National Retail Federation
The Voice of Retail Worldwide

STATEMENT OF THE

NATIONAL RETAIL FEDERATION

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

COMMITTEE ON FINANCIAL SERVICES

"CREDIT CARD DATA PROCESSING: HOW SECURE IS IT?'

THURSDAY, JULY 21, 2005

Good morning I am Mallory Duncan, Senior Vice President and General Counsel for the National Retail Federation. I appreciate the opportunity to testify at today's hearing. By way of background, the National Retail Federation is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet and independent stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.4 million U.S. retail establishments, more than 23 million employees - about one in five American workers - and 2004 sales of $4.1 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations.

The Nature of the Problem

There has been a substantial increase in reported incidents of identity theft over the past several years. Precise year-to-year comparisons among the competing estimates are difficult to make because the methods of measuring prevalence, awareness of the issue and the definition of the problem itself differ significantly among those who are reporting and those keeping track. In May, 2003 the Department of Justice, in conjunction with the Solicitor General of Canada, issued a Public Advisory and Special Report to retailers on identity theft. At that time, the Department of Justice indicated that identity theft complaints to the Federal Trade Commission ("FTC") had increased fivefold since 2000, from

31,117 to 161, 819 in 2002. The Canadian PhoneBusters National Call Centre received 7,629 identity theft complaints in 2002 with reported total losses of $8.5 million. The advisory further indicated that two major Canadian credit bureaus received approximately 1,400 to 1,800 complaints of identity theft per month. On February 1, 2005, the FTC released its 2004 complaint numbers. Again, reports of identity theft continued to climb, reaching 215,093 in 2003 and 246,570 in 2004[1]. Recently, the FTC completed a national survey in which it projected approximately ten million people experienced identity theft within the past year. Even larger numbers have been published elsewhere.

As striking as these figures are, it is important to recognize that the frauds they reflect comprise a variety of activities, not all of which are true identity theft and not all of which are susceptible to the same analysis or solutions. For purposes of today's hearing, let me explain what we mean when we speak about true identity theft.

Compared to fifty years ago, we live in a mobile, fragmented society. Relatively few of us reside in the community in which we were born, and even fewer of us have neighbors or shopkeepers who've known us since birth. Although passports and other such documents have long existed, day-to-day proof of our identity has shifted from being something that was known or vouched for by others to something that is inferred from documentation and our knowledge of relatively obscure facts. In today's world, individual identifiers such

[1] The FTC further breaks down identity theft complaints to include: credit card fraud (28 percent), phone or utilities fraud (19 percent), bank fraud (18 percent), loan fraud (5 percent), other identity theft (22 percent), government documents or benefits fraud (8 percent), employee-related fraud (13 percent) and attempted identity theft (8 percent).

drivers licenses or social security numbers, and quick recall of personally-related facts such as date of birth, mother's maiden name, and office telephone numbers, substitute for actual proof of identity. This is an accommodation we've made in order to allow millions of us to routinely travel thousands of miles from our birthplaces to work, to relocate and to recreate. This system worked reasonably well so long as the identifiers were unique, the personally-related facts were largely buried, and the pace of business was slow.

True identity theft occurs when someone appropriates another individual's identifying data for the purpose of secretly assuming that person's identity. For example, a thief, by the name of Susan Kelly may decide to become "Sue Kelly." The thief may associate the real Sue Kelly's name, social security number, date of birth and other facts with her, Susan Kelly's "new" address. The thief may go on to obtain a driver's license, open credit and checking accounts, purchase a car, even buy a condominium, using Sue Kelly's excellent credit history. So long as the thief keeps up her payments or doesn't otherwise draw attention to herself, it might be months or years before anyone discovers the fraud, if ever.

These true identity thefts are the frauds that make the crime of that name so frightening. At some point the thief may decide to start writing bad checks and to stop making payments on the car, the house or the cards, stiffing the creditors and potentially ruining the victim's consumer report. It could take months or years for the victim to recover her or his good name. Worse, if the thief is not apprehended, there is always the possibility that she or he will lay low, wait one,

two or seven years, and attempt to repeat the process again. The victim may need to be ever vigilant.

In contrast, much of what is commonly referred to as identity theft is, in fact, relatively straightforward credit card fraud. While retailers do not by any means make light of it, and it can be a problem for those affected, it is much closer to a serious nuisance than it is to the horror of true identity theft. Equally important, Congress has already provided many of the tools victims need for its correction.

In a typical credit card fraud someone obtains all or enough information from an individual's credit or debit card in order to accomplish a transaction. The crime could be as simple as an attendant making two impressions of a credit card on an embossing machine, and submitting both for payment; or it could be as sophisticated as capturing all of the critical data from a card and creating a phony "cloned copy" of the card that is sold on the black market or used for an intensive shopping spree. Regardless, the individual who's card information was taken will be made aware of the fraud either through a contact from the credit card company, inquiring as to the suspicious activity, or when the monthly statement arrives detailing the fraudulent charges. Congress has provided (under Truth-in-Lending, Fair Credit Billing Act) that the consumer may challenge those charges and, unless the consumer were contributorially negligent, the consumer is held harmless for the loss. Either the retailer or the card issuer bears the burden. I would like to repeat that point: retailers typically bear the financial burden of credit card fraud.

With these distinctions in mind, it is clear that the incidence of identity theft is considerably different than some of the numbers that are cited. While reported cases have been in the hundreds of thousands, even if one accepts the ten million cases estimated by the FTC, on closer analysis it turns out that two-thirds of those are not truly identity theft.

What also is important to note about these two types of fraud is that the remedies are quite different. Credit card fraud is usually a one-off event. Once the crime has been discovered it is relatively simple to stop the thief from continuing to victimize that individual by closing the account and reopening a new account with a different number. Within a matter of hours or minutes the thief's card information essentially becomes useless. On the other hand, when true identity theft occurs, it is not a simple matter to change an individual's social security number, date of birth or mother's maiden name. The tools to commit the crime again remain in the thief's possession. It is for these reasons that it is important Congress not lump these very different frauds into the same basket. If society has limited resources that it can devote to fighting crime, then we ought to tilt toward using those resources to help those confronted with the most serious consequences, e.g. true identity theft.

Thus, fraud alerts and regular monitoring of consumer reports might makes greater sense when there has been true identity theft. They put up a red flag to those who would grant credit, informing them that a thief has been impersonating the consumer and can provide the consumer with an opportunity

to ensure that new accounts are not being opened in his or her name. On the other hand, consumer report monitoring, for example, is virtually useless at detecting credit card fraud. The thief is not opening new accounts, he is running up charges on existing accounts; charges that the consumer can eliminate at month's end. Therefore, it makes little sense to expend huge amounts of money to provide regular monitoring to those who have experienced unauthorized use of their credit cards when those funds might better be spent on other protections, such as even more sophisticated neural networks or improved payment systems.

This underscores another important point. In contrast to the identity theft-sensitive information discussed above, most of the information retailers maintain is fairly innocuous. They may maintain some credit card data. In general, when a purchase is made on a card, the retailer transmits all of the necessary card data to its acquiring bank or processor for authorization. Once authorization is received retailers are directed to eliminate all but the most basic credit card information from their files. Basic credit card information (name, account number and expiration date, but absent the information necessary to create a cloned card) may be retained in order to facilitate customer returns. Beyond basic card data, and independent of the financial services systems, information about prior purchases or customer preferences (e.g. sizes, colors or styles) may be maintained in order to provide more personalized service. Mailing addresses may be used to speed future transactions and for quality or security purposes.

From an identity theft perspective all information is not equal, and none of the foregoing is directly implicated. We have an exceedingly complex economy.

The use of different types of information poses greatly differing levels of risk and provides differing levels of benefit to consumers. If identity theft prevention is the goal, Congress should be especially sensitive to the associated costs and benefits of the type of information at issue, and its usage in various environments, so as to avoid painting with too broad a brush.

What Has Been Done

The growing reports of identity theft led to a significant amount of testimony before the House Financial Services Committee in 2002 and 2003, as part of a series of hearings held on the reauthorization of the Fair Credit Reporting Act. Indeed, this Committee went on to establish many new protections for identity theft victims in the Fair and Accurate Transactions Act (FACTA), including the right to block fraudulent information on their credit reports and the creation of new fraud alert systems so that new credit would not so readily be extended to identity thieves. After extensive rulemaking, many of these new rules and protections are now just coming on-line, and there is still much work left to do.

As members of the Committee are aware, shortly before the FACT Act was signed into law, a new California statute was enacted requiring the public disclosure of security breaches under certain circumstances. This law, and the data security events that it has caused to be made public, has brought the issues of data security, consumer privacy and identity theft to the public's attention like

never before. These highly publicized stories appear to have eclipsed somewhat the important work Congress did to protect consumers just a year and a half ago. The reported breaches have ranged from the mistaken sale of thousands of files full of sensitive personal information to criminals posing as legitimate businesses, as in the case of ChoicePoint, to encrypted data tapes containing account information literally disappearing in the cargo hold of a plane, as in the case of Bank of America. In the retail sector, reported cases have involved criminals attacking and hacking into computer systems in order to steal customer credit card information.

What is telling about the recent media stories is that almost all the large disclosures have involved credit card data, not identity theft data. In some ways this suggests it currently may be easier for thieves to obtain the less damaging type of information. Nevertheless, a great deal of attention has been focused on means of reducing the incidence of credit card fraud. Over the course of this summer, substantial numbers of merchants are expected to come on line with Visa and MasterCard's new card security program. Begun several years ago to protect credit card purchases on the then nascent Internet, the card association are extending the security requirement to cover virtually all credit card transactions.

The FTC recently entered into a proposed settlement with B.J.'s Wholesale Club as the result of one these system attacks in late 2003 that resulted in millions in fraudulent charges on their customers' credit accounts.

Part of the settlement alleges that B.J.s was in violation of the type of bank security rules that I described above. The B.J.'s case, however, has been something of an anomaly, and other reported retail computer attacks, to our knowledge, have been discovered and managed before they have resulted in significant losses.

Retail Specific Difficulties

From a retailer perspective, there are some areas where the damage caused by true identity theft and that caused by credit card fraud can overlap. If a true identity thief is able to apply for and obtain a credit card, he may use it to make purchases, either remotely or in person. Depending on the circumstances the retailer innocently accepting the card may be forced to absorb the cost of the fraud. On the other hand, when full file credit card data is stolen from an entity and enough information is captured to clone that card (create an exact duplicate with an active magnetic strip), it is often difficult for a merchant, or any other entity, to detect that a card used at point of sale is indeed a fraudulent card. Once the magnetic strip is duplicated it allows the cloned card to run over electronic authorizations channels just like an authentic card, and unless the original card has been reported lost or stolen, or the card companies' neural networks have detected potentially fraudulent spending patterns, it will be approved just like an authentic transaction. Nevertheless, the merchant may or may not be responsible for the transaction depending on a variety of factors. As mentioned above, it is the card companies, who are in the best position to

develop these fraud detection systems. They “see” a broader range of transactions, have a larger body of customer shopping pattern experience, and thus are more likely first to discover that a card number breach or cloning pattern has occurred.

This is important because by and large retailers are not in a position to bargain as to the terms of card acceptance. Penalties, requirements and ever-changing rules are largely dictated as a condition of acceptance. While the card systems are premised on mutual benefit, most of the leverage is on one side. We ask that you carefully consider any legislative changes so as not to further disadvantage those who already pay so large a portion of the cost of fraud. To the extent Congress directs its attention to the core problem, true identity theft, this is less likely to occur.

In summary, identity theft is fairly focused, but harmful, form of fraud. Proof of identity has become a more elusive quality at the same time that our society has invested greater amounts of trust in its veracity. Viewed objectively and from a distance our credit granting system seems miraculously facile. Families receive high-quality meals in exchange for a swipe of plastic. Vacationers are able to take possession of cars hundreds of miles from home merely by presenting out-of-state documents and cards. Individuals are able to secure funds to purchase their homes from bankers they have never before met. These benefits flow not from the credit cards, but rather from the trust our society invests in the identities of the persons seeking credit. If we are to preserve

these benefits, society should crackdown on those who would abuse that trust by appropriating the core incidents of identity. With the passage of the FACT Act Congress has begun to provide tools to those who have been victimized; it now should provide funding to ferret out and prosecute those who make the use of such tools necessary.

Thank you for the opportunity to appear here today. I would be happy to answer your questions.